

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-187357

(43)Date of publication of application : 04.07.2003

(51)Int.Cl. G08B 25/08
 B60R 25/10
 G08B 13/00
 G08B 25/00
 G08B 25/04
 G08B 25/10
 H04Q 9/00

(21)Application number : 2001-381679

(71)Applicant : PIONEER ELECTRONIC CORP

(22)Date of filing : 14.12.2001

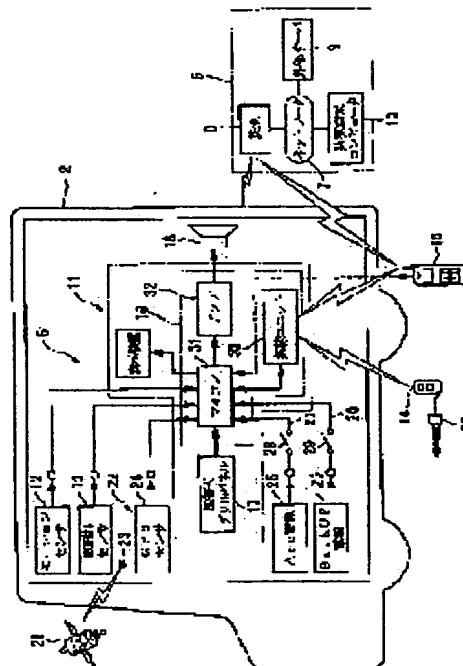
(72)Inventor : NONAKA YOSHIYA

(54) DEVICE, SYSTEM AND METHOD FOR PREVENTING THEFT AND PROGRAM THEREOF

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a theft preventing device whose configuration is simplified and whose general purpose property is improved, and to provide a theft preventing method, a theft prevention system and their program.

SOLUTION: Electronic equipment 11 having a microcomputer 31 that controls the operation of a reproducing device, etc., for reproducing sound data is provided in a vehicle 2. A radio unit 33 is connected to the microcomputer 31. When the electronic equipment 11 is in an operating state by the power supply from the vehicle 2, the radio unit 33 does not receive an authentication code from an authentication transmitter-receiver 14. If the authentication code does not coincide with authentication data proper to an owner and stored in the electronic equipment 11, information showing that abnormality has occurred is outputted.



LEGAL STATUS

[Date of request for examination]

02.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

【特許請求の範囲】

【請求項 1】 移動体に取り付けられ、この移動体から供給される電力により起動される機器と、前記機器に記憶された所有者固有の認証コードと同等の認証コードが記憶されるとともに、前記機器に対しその認証コードの信号を送信することが可能な認証コード記憶送信手段と、前記機器が起動状態にあるときに前記認証コード記憶送信手段から送信される認証コードの信号を受信することが可能な認証コード受信手段と、前記認証コード受信手段が受信した認証コードと前記機器に記憶された前記所有者固有の認証コードとが一致した場合に前記移動体の正規の所有者が前記移動体を利用していると判断する制御手段と、を具備したことを特徴とする盗難防止装置。

【請求項 2】 請求項 1 に記載の盗難防止装置において、前記機器は、前記移動体から供給される電力により起動される機器本体と、この機器本体に着脱可能な操作手段とを備え、前記制御手段は、前記認証コード受信手段が受信した認証コードと前記機器に記憶された前記所有者固有の認証コードとが一致し、かつ前記操作手段が前記機器本体に装着された場合に前記移動体の正規の所有者が前記移動体を利用していると判断することを特徴とする盗難防止装置。

【請求項 3】 請求項 1 に記載の盗難防止装置において、異常が発生したことを示す情報を出力する異常発生出力手段を具備し、前記制御手段は、前記機器が起動状態にあるときに前記認証コード受信手段が前記認証コード記憶送信手段から送信される認証コードの信号を受信していない、または前記認証コード受信手段が受信する認証コードの信号が前記機器に記憶された所有者固有の認証コードと一致しないと判断した場合には、前記異常発生出力手段を制御して前記情報を出力させることを特徴とする盗難防止装置。

【請求項 4】 請求項 2 に記載の盗難防止装置において、異常が発生したことを示す情報を出力する異常発生出力手段を具備し、前記制御手段は、前記機器本体が起動状態にあるときに前記認証コード受信手段が前記認証コード記憶送信手段から送信される認証コードの信号を受信していない、または前記認証コード受信手段が受信する認証コードの信号が前記機器本体に記憶された所有者固有の認証コードと一致しない、または前記操作手段が前記機器本体に装着されていないと判断した場合には、前記異常発生出力手段を制御して前記情報を出力させることを特徴とする

盗難防止装置。

【請求項 5】 請求項 3 または 4 に記載の盗難防止装置において、前記異常発生出力手段は、異常が発生したことを示す情報を音として出力することを特徴とする盗難防止装置。

【請求項 6】 請求項 3 または 4 に記載の盗難防止装置において、前記異常発生出力手段は、異常が発生したことを示す情報を無線送信媒体にて外部に送信することにより出力することを特徴とする盗難防止装置。

【請求項 7】 請求項 6 に記載の盗難防止装置において、前記機器は、前記移動体の現在位置を示す位置情報を取得する機能を具備し、前記異常発生出力手段は、異常が発生したことを示す情報とともに前記位置情報を送信することを特徴とする盗難防止装置。

【請求項 8】 請求項 3、4、6 および 7 のいずれかに記載の盗難防止装置と、

20 この盗難防止装置から送信される異常が発生したことを示す情報を取得し、この取得した情報を送信する外部サーバと、を具備したことを特徴とする盗難防止システム。

【請求項 9】 請求項 7 に記載の盗難防止装置と、この盗難防止装置から送信される異常が発生したことを示す情報と前記移動体の現在位置を示す位置情報とを取得し、前記異常が発生したことを示す情報を取得した以降に取得する位置情報を逐次更新するとともに、この更新された位置情報を送信する外部サーバと、を具備したことを特徴とする盗難防止システム。

30 【請求項 10】 移動体に取り付けられた機器がこの移動体から供給される電力により起動されたことを検出する工程と、前記機器が起動状態にあるときに外部から送信される認証コードの受信を可能とする工程と、前記機器が起動状態にあるときに外部から送信される認証コードを受信していない、または受信した認証コードが前記機器に記憶された所有者固有の認証コードと一致しない場合には、異常が発生したことを示す情報を出力させる制御工程とを有したことを特徴とする盗難防止方法。

40 【請求項 11】 移動体に取り付けられ、操作手段を着脱可能とする機器本体がこの移動体から供給される電力により起動されたことを検出する工程と、前記機器本体が起動状態にあるときに外部から送信される認証コードの受信を可能とする工程と、前記機器本体が起動状態にあるときに外部から送信される認証コードを受信していない、または受信した認証コードが前記機器本体に記憶された所有者固有の認証コードと一致しない、または前記操作手段が前記機器本体に

装着されていない場合には、異常が発生したことを示す情報を出力させる制御工程とを有したことを特徴とする盗難防止方法。

【請求項12】 請求項10または11に記載の盗難防止方法をコンピュータに実行させることを特徴とする盗難防止プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、移動体等の盗難を防止する盗難防止装置、盗難防止システム、盗難防止方法およびそのプログラムに関する。

【0002】

【背景技術】従来、この種の盗難防止装置として、例えば、図5のブロック図に示すような構成が知られている。この図5に示す盗難防止装置41は、例えば、移動体としての自動車などの車両42に装着される。盗難防止装置41は、オーディオ装置やナビゲーションシステム装置などの電子機器43と、モーションセンサ44と、窓割れセンサ45と、ドアロック解除センサ46と、ドア開閉センサ47とを備えている。電子機器43は、機器本体48と、この機器本体48に着脱可能に装着される操作手段としての脱着式グリルパネル49と、スピーカ50と、液晶ディスプレイ装置などの表示装置51とを備えている。

【0003】機器本体48は、マイクロコンピュータ52と、アンプ53と、CD（Compact Disk）などの記憶媒体に記憶されている情報信号を読み取り、所定の信号処理を施してアンプ53や表示装置に供給するための図示しない再生装置などを備えている。マイクロコンピュータ52は、アンプ53や表示装置、再生装置などの動作制御を司る。アンプ53は、再生装置から供給される信号処理が施された音声信号を増幅してスピーカ50に供給する。さらに、アンプ53は、マイクロコンピュータ52の制御によりアラーム音などの音データを生成してスピーカ50に供給する。

【0004】また、機器本体48は、車両42に搭載されたアクセサリ（Acc）電源55およびバックアップ（BackUP）電源56から電力が供給されて起動状態とされる。なお、Acc電源55と機器本体48とを結ぶ電力供給ライン57には、アクセサリスイッチ（Accスイッチ）58が設けられている。また、バックアップ電源56と機器本体48とを結ぶ電力供給ライン59には、バックアップスイッチ60が設けられている。

【0005】そして、車両42の搭乗者がAccスイッチ58をオンさせると、それに同期してバックアップスイッチ60がオフされ、Acc電源55からの電力が機器本体48に供給される。また、車両42の搭乗者がAccスイッチ58をオフさせると、それに同期してバックアップスイッチ60がオンされ、バックアップ電源56からの電力が機器本体48に供給される。なお、車両

42が停止中のときは、バックアップ電源56からの電力が機器本体48のマイクロコンピュータ52のみに供給される。

【0006】スピーカ50は、アンプ53から供給される音声信号や音データを音として出力する。表示装置は、マイクロコンピュータ52の制御により再生装置から供給される情報を画像として液晶ディスプレイなどの表示パネルに表示する。例えば、電子機器43がナビゲーションシステム装置である場合には、再生装置から供給される地図情報などを表示パネルに表示する。

【0007】脱着式グリルパネル49は、各種操作スイッチなどを備えている。また、この脱着式グリルパネル49は、機器本体48に設けられた図示しない脱着機構により着脱可能となっている。さらに、この脱着式グリルパネル49には、機器本体48と電氣的に接続状態とする図示しない接続端子が設けられている。すなわち、脱着式グリルパネル49が機器本体48に装着されると、接続端子が機器本体48側の接続端子に接合されることにより脱着式グリルパネル49が通電状態となる。

【0008】そして、機器本体48からの電力が接続端子を介して脱着式グリルパネル49に供給されて起動状態となる。この起動状態から車両42の搭乗者が操作スイッチを操作することで、その操作に応じて操作信号が接続端子を介して機器本体48に供給され、上述した再生装置などの各種動作が実施される。

【0009】また、接続端子は、脱着式グリルパネル49が機器本体48に対し着脱されたことを検知する図示しないデタッチセンサが設けられている。そして、マイクロコンピュータ52は、このデタッチセンサの検知を得ることにより、脱着式グリルパネル49が機器本体48に対して着脱されたことを認識する。なお、脱着式グリルパネル49は、車両42の搭乗者が降車するときに機器本体48から取り外される。そして、電子機器43を使用不能状態とすることにより、電子機器43の盗難を未然に防止している。

【0010】モーションセンサ44は、車両42の不審（異常）な動きを検知する。モーションセンサ44は、例えば、車両42のサスペンションに設置され、通常、搭乗者の乗降動作に伴い停止中の車両42が受ける振動などのレベルをデータとして管理し、車両42がそのレベルを超える振動など、例えば、車両の前部または後部が持ち上げられたときに受ける振動などを受けたことを検知すると、不審（異常）な動きと判断して電子機器43のマイクロコンピュータ52に検知信号を出力する。

【0011】窓割れセンサ45は、車両42に設けられた図示しないドアウィンド、フロントガラス、リアガラスなどが割れたことを検知する。窓割れセンサ45は、例えばドアウィンド、フロントガラス、リアガラスなどに埋め込まれており、それらが外部から過度の衝撃を受けたことを検知するとそれらが割れたと判断して電子機

器 4 3 のマイクロコンピュータ 5 2 に検知信号を出力する。

【0012】ドアロック解除センサ 4 6 は、車両 4 2 の図示しないドアのロックが解除されたことを検知する。ドアロック解除センサ 4 6 は、例えば、車両 4 2 のドア内部の図示しないドアロック機構に設けられており、そのドアロック機構の動作に基づきドアのロックが解除されたことを検知する。そして、ドアロック解除センサ 4 6 は、電子機器 4 3 のマイクロコンピュータ 5 2 に検知信号を出力する。

【0013】ドア開閉センサ 4 7 は、車両 4 2 のドアが開閉されたことを検知する。ドア開閉センサ 4 7 は、例えば、ドアを開閉させるための図示しないドア開閉機構に設けられており、そのドア開閉機構の動作に基づきドアの開閉状態を検知する。そして、ドア開閉センサ 4 7 は、電子機器 4 3 のマイクロコンピュータ 5 2 に検知信号を出力する。

【0014】上述した盗難防止装置 4 1 では、電子機器 4 3 のマイクロコンピュータ 5 2 がモーションセンサ 4 4 や窓割れセンサ 4 5 からの検知信号を受けると、車両 4 2 に異常が発生したと判断してアンブ 5 3 を制御する。そして、アンブ 5 3 は、マイクロコンピュータ 5 2 の制御に基づきアラーム音などの音声データを生成してスピーカ 5 0 に供給する。スピーカ 5 0 は、アンブ 5 3 から供給された音データを音として出力する。

【0015】また、盗難防止装置 4 1 は、電子機器 4 3 のマイクロコンピュータ 5 2 がドアロック解除センサ 4 6 とドア開閉センサ 4 7 からの検知信号を受けると、Acc スイッチ 5 8 がオン状態になってから所定時間経過しても脱着式グリルパネル 4 9 が機器本体 4 8 に装着されない、すなわちデタッチセンサによる機器本体 4 8 への装着検知が得られないと認識すると、マイクロコンピュータ 5 2 はアンブ 5 3 を制御し、スピーカ 5 0 からアラーム音などの音を出力させる。

【0016】このようにして、従来の盗難防止装置 4 1 では、車両 4 2 の正規の所有者以外の侵入者が車両 4 2 に搭乗したと判断してアラーム音などの音を出力している。そして、移動体である車両 4 2 や、その車両 4 2 に搭載された電子機器 4 3 の盗難を防止している。

【0017】ところで、移動体である車両 4 2 は、利用者の好みや利用形態を考慮して多くの種類が存在する。また、ドアの開閉機構やドアロック機構は車両 4 2 の種類によって異なるため、予め装備されたドアロック解除センサ 4 6 やドア開閉センサ 4 7 から送信される信号が車種によって異なるように設計されている。このため、従来の盗難防止装置 4 1 は、その車種によって異なる信号のそれぞれを解析し、それらの信号に応じた汎用性のある機能にしなければならず、設計、開発上極めて困難を奏する。

【0018】

【発明が解決しようとする課題】上述したように、従来の盗難防止装置 4 1 では、多種の車両 4 2 のドアロック解除センサ 4 6 やドア開閉センサ 4 7 から送出される異なる信号に応じた汎用性のあるものにしなければならず、設計、開発が極めて困難を奏するという不具合があり、車種によっては、盗難防止装置 4 1 の取付を見合わせなければならないということも懸念される。

【0019】本発明は、このような問題点に鑑みなされたものであって、簡易な構成により汎用性を実現することのできる盗難防止装置、盗難防止システム、盗難防止方法およびそのプログラムを提供することを目的とする。

【0020】

【課題を解決するための手段】請求項 1 記載の発明は、移動体に取り付けられ、この移動体から供給される電力により起動される機器と、前記機器に記憶された所有者固有の認証コードと同等の認証コードが記憶されるとともに、前記機器に対しその認証コードの信号を送信することが可能な認証コード記憶送信手段と、前記機器が起動状態にあるときに前記認証コード記憶送信手段から送信される認証コードの信号を受信することが可能な認証コード受信手段と、前記認証コード受信手段が受信した認証コードと前記機器に記憶された前記所有者固有の認証コードとが一致した場合に前記移動体の正規の所有者が前記移動体を利用していると判断する制御手段とを具備したことを特徴とする盗難防止装置である。

【0021】請求項 2 記載の発明は、請求項 1 に記載の盗難防止装置において、前記機器は、前記移動体から供給される電力により起動される機器本体と、この機器本体に着脱可能な操作手段とを備え、前記制御手段は、前記認証コード受信手段が受信した認証コードと前記機器に記憶された前記所有者固有の認証コードとが一致し、かつ前記操作手段が前記機器本体に装着された場合に前記移動体の正規の所有者が前記移動体を利用していると判断することを特徴とする。

【0022】請求項 3 記載の発明は、請求項 1 に記載の盗難防止装置において、異常が発生したことを示す情報を出力する異常発生出力手段を具備し、前記制御手段は、前記機器が起動状態にあるときに前記認証コード受信手段が前記認証コード記憶送信手段から送信される認証コードの信号を受信していない、または前記認証コード受信手段が受信する認証コードの信号が前記機器に記憶された所有者固有の認証コードと一致しないと判断した場合には、前記異常発生出力手段を制御して前記情報を出力させることを特徴とする。

【0023】請求項 4 記載の発明は、請求項 2 に記載の盗難防止装置において、異常が発生したことを示す情報を出力する異常発生出力手段を具備し、前記制御手段は、前記機器本体が起動状態にあるときに前記認証コード受信手段が前記認証コード記憶送信手段から送信され

10

20

30

40

50

る認証コードの信号を受信していない、または前記認証コード受信手段が受信する認証コードの信号が前記機器本体に記憶された所有者固有の認証コードと一致しない、または前記操作手段が前記機器本体に装着されていないと判断した場合には、前記異常発生出力手段を制御して前記情報を出力させることを特徴とする。

【0024】請求項5記載の発明は、請求項3または4に記載の盗難防止装置において、前記異常発生出力手段は、異常が発生したことを示す情報を音として出力することを特徴とする。

【0025】請求項6記載の発明は、請求項3または4に記載の盗難防止装置において、前記異常発生出力手段は、異常が発生したことを示す情報を無線送信媒体にて外部に送信することにより出力することを特徴とする。

【0026】請求項7記載の発明は、請求項6に記載の盗難防止装置において、前記機器は、前記移動体の現在位置を示す位置情報を取得する機能を具備し、前記異常発生出力手段は、異常が発生したことを示す情報とともに前記位置情報を送信することを特徴とする。

【0027】請求項8記載の発明は、請求項3、4、6および7のいずれかに記載の盗難防止装置と、この盗難防止装置から送信される異常が発生したことを示す情報を取得し、この取得した情報を送信する外部サーバとを具備したことを特徴とする盗難防止システムである。

【0028】請求項9記載の発明は、請求項7に記載の盗難防止装置と、この盗難防止装置から送信される異常が発生したことを示す情報と前記移動体の現在位置を示す位置情報とを取得し、前記異常が発生したことを示す情報を取得した以降に取得する位置情報を逐次更新するとともに、この更新された位置情報を送信する外部サーバとを具備したことを特徴とする盗難防止システム。

【0029】請求項10記載の発明は、移動体に取り付けられた機器がこの移動体から供給される電力により起動されたことを検出する工程と、前記機器が起動状態にあるときに外部から送信される認証コードの受信を可能とする工程と、前記機器が起動状態にあるときに外部から送信される認証コードを受信していない、または受信した認証コードが前記機器に記憶された所有者固有の認証コードと一致しない場合には、異常が発生したことを示す情報を出力させる制御工程とを有することを特徴とする盗難防止方法である。

【0030】請求項11に記載の発明は、移動体に取り付けられ、操作手段を着脱可能とする機器本体がこの移動体から供給される電力により起動されたことを検出する工程と、前記機器本体が起動状態にあるときに外部から送信される認証コードの受信を可能とする工程と、前記機器本体が起動状態にあるときに外部から送信される認証コードを受信していない、または受信した認証コードが前記機器本体に記憶された前記所有者固有の認証コードと一致しない、または前記操作手段が前記機器本体

に装着されていない場合には、異常が発生したことを示す情報を出力させる制御工程とを有することを特徴とする盗難防止方法。

【0031】請求項12に記載の発明は、請求項10または11に記載の盗難防止方法をコンピュータに実行させることを特徴とする盗難防止プログラムである。

【0032】

【発明の実施の形態】以下に、本発明の一実施形態を図面に基いて説明する。

10 【0033】図1は、本実施形態の盗難防止システムの概略構成を示す模式図である。この図1において、盗難防止システム1は、インターネットやイントラネットなどのコンピュータネットワーク技術を用いて実現されるもので、移動体である、例えば、車両2の盗難や車上荒らしなどを防止するためのシステムである。そして、この盗難防止システム1は、車両2に搭載された盗難防止装置5と、防犯ネットワーク6とを備えている。

【0034】防犯ネットワーク6は、イントラネットやインターネットなどの通信回路網にて構成されたネットワーク7を介して接続された基地局8と、監視センタに設置された外部サーバ9と、防犯センタに設置させた防犯端末コンピュータ10とを備えている。基地局8は、後述する盗難防止装置5からの異常が発生したことを示す情報をネットワーク7を介して外部サーバ9に送信する。外部サーバ9は、ネットワーク7を介して防犯センタの防犯端末コンピュータ10に異常を報知する。なお、防犯センタは、例えば、公的機関である警察の他に警備会社などの民間の機関でもよく、異常に対処するいずれの機関でもよい。

30 【0035】外部サーバ9は、図示しない演算処理装置と、通報装置と、図2に示すような後述する位置情報データベースとを備えている。通報装置は、有線や無線などにより防犯端末コンピュータ10に異常を報知するための信号を出力する。演算処理装置は、基地局8から異常が発生したことを示す情報を受信したときに異常を通報するための信号を出力させるべく通報装置を制御する。

40 【0036】また、位置情報データベースは、基地局8を介して盗難防止装置5から送信される車両2の現在位置を示す位置情報を蓄積するものである。この位置情報データベースは、図2に示すように、車両2からの登録された車両2の固有の番号に対応して、車両2の現在位置を示す緯度経度情報を1つのレコードとして記録した構造とされている。各レコードは、車両2からの現在の位置情報を取得する毎に更新され、図2にも示すように、各レコードには、車両2の登録番号、位置情報である緯度経度情報の他、更新日、更新時間を記録するフィールドが設けられている。基地局8から異常が発生したことを示す情報が送信されると、それと共に送信されてくる位置情報がリアルタイムに更新される。そして、演

算処理装置の制御により、この位置情報を異常を報知する信号とともに防犯センタの防犯端末コンピュータ10に送信する。

【0037】防犯センタの防犯端末コンピュータ10には、図3に示すような地図情報を表示する図示しない表示装置が設けられている。そして、外部サーバ9から送信された位置情報に基づき、車両2の現在位置をその地図情報に重畳表示させることで、盗難されるおそれのある車両2の現在位置をリアルタイムで把握することができるので、迅速に対応することが可能となる。

【0038】盗難防止装置5は、図1に示すように、電子機器11と、モーションセンサ12と、窓割れセンサ13と、認証コード記憶送信手段としての認証送受信機14と、携帯電話機などの移動通信端末15とを備えている。

【0039】電子機器11は、機器本体16と、この機器本体16に着脱可能に装着される操作手段としての脱着式グリルパネル17と、スピーカ18と、液晶ディスプレイや有機ELディスプレイなどの表示装置19とを備えている。

【0040】機器本体16は、例えば、車両2における図示しない運転席と助手席との間に位置するダッシュボードに配設されている。また、この機器本体16は、人工衛星21からの電波を受信するGPS(Global Positioning System)受信機22が接続されている。このGPS受信機22は、GPSアンテナ23とGPSセンサ24とを備え、GPSアンテナ23にて人工衛星21からの電波を受信し、GPSセンサ24にて受信した電波の状態に基づいて車両2の現在位置を計測する。

【0041】また、機器本体16は、車両2に搭載されたアクセサリ(Acc)電源25またはバックアップ(BackUP)電源26から電力供給を受ける。なお、Acc電源25と機器本体16とを結ぶ電力供給ライン27aには、アクセサリスイッチ(Accスイッチ)28が設けられている。また、バックアップ電源26と機器本体16とを結ぶ電力供給ライン27bには、バックアップスイッチ29が設けられている。

【0042】そして、後述する車両キー30の操作により、Accスイッチ28がオンされて機器本体16が起動状態になるとともに、バックアップスイッチ29がオフとなり、さらに車両キー30が継続して操作されることにより車両2の図示しないエンジンが始動される。また、車両キー30の操作によりエンジンが停止しAccスイッチ28がオフされるとバックアップスイッチ29がオンされ、機器本体16にバックアップ電源26から電力が供給されて、後述するマイクロコンピュータ31のみが起動状態とされる。

【0043】機器本体16は、制御手段としてのマイクロコンピュータ31、アンプ32、認証コード受信手段としての無線ユニット33、音楽情報などを記録したC

D(Compact Disk)や地図情報などを記録したCD-ROM(Read Only Memory)などを再生する再生装置などを備えている。そして、機器本体16は、Acc電源25から電力供給を受けて起動状態とされる。なお、上述したGPS受信機22と地図情報などを記録したCD-ROMなどを再生する再生装置とによりナビゲーションシステムが構成され、このナビゲーションシステムにより車両2の現在位置を示す位置情報を地図情報と共に表示装置19に表示させる。

【0044】マイクロコンピュータ31は、アンプ32、無線ユニット33、表示装置19、上記した再生装置などの動作制御を司る。そして、モーションセンサ12と窓割れセンサ13からの検知信号を受けて、それらの検知信号に応じた制御処理を司るとともに、GPS受信機22により得られた車両2の現在位置を示す位置情報を図示しない内蔵メモリに記憶し、必要に応じて出力する。

【0045】また、マイクロコンピュータ31には図示しない内蔵メモリが備えられており、その内蔵メモリには車両2を所有する所有者(原則として車両2の車検を登録している登録者とされる)であることを示す所有者固有の認証コードが予め記憶されている。この認証コードは、例えば、電子機器11が配設された車両2を購入するとき、または電子機器11の機器本体16を車両2に配設するときなどにそれらの販売元により予め設定登録されるものであり、設定された以降、所有者が簡易に変更することができないものとされている。

【0046】さらに、マイクロコンピュータ31は、後述する無線ユニット33からの認証コードを示す信号を受けて、内蔵メモリに記憶された認証コードとの照合を実施し、その結果に基づき移動通信端末15や無線ユニット33を制御する。

【0047】アンプ32は、再生装置などから供給される音楽情報などの音声信号を増幅してスピーカ18に供給する。また、アンプ32は、マイクロコンピュータ31からの制御によりアラーム音などの音データを生成してスピーカ18に供給する。つまり、モーションセンサ12や窓割れセンサ13からの検知信号を受けたとき、マイクロコンピュータ31はアンプ32を制御して音データを生成させ、スピーカ18に供給させる。

【0048】無線ユニット33は、近距離無線通信により電気信号を伝送する近距離無線送受信機、例えば、ブルーツース(Bluetooth:登録商標)送受信機とされている。ここで、ブルーツース送受信機とは、例えば、LSI(Large Scale Integration)を主体として構成され、近距離無線通信技術規格であるBluetoothに基づく近距離無線通信機能を有し、他のブルーツース送信機と近距離無線によるデータ通信を実施するものである。具体的には、Bluetoothによる通信公式には、スレーブマスタ方式が適用され、処理内容に応じて、周波数ホッピ

ングパターンを決定するマスタ機器と、このマスタ機器に制御される送信相手のスレーブ機器とに分かれる。そして、かかるマスタ機器は、半径約10m内に存在するスレーブ機器を認識した場合、お互いの機器が有する専用のIDナンバを交換して確認した後、乱数を発生させて、マスタ機器とスレーブ機器との間におけるリンクキー（暗号キー）を生じるといった認証処理を実施する。かかる認証処理により、マスタ機器とスレーブ機器との間の接続、すなわち近距離無線通信による電気信号の伝送路が確立され、データ通信が可能となる。ここで、無線

【0049】一方、脱着式グリルパネル17は、機器本体16の前面を開閉可能でかつ機器本体16に着脱可能に取り付けられている。この脱着式グリルパネル17には、前面に図示しない各種スイッチなどが複数配設されている。これらスイッチを搭乗者が入力操作することにより、機器本体16の動作が設定入力される。また、脱着式グリルパネル17には、背面側に図示しない係止手段が設けられている。この係止手段は、機器本体16の前面に設けられた図示しない係合手段に係脱可能に係合され、脱着式グリルパネル17を機器本体16の前面の所定の位置に装着させる。

【0050】さらに、脱着式グリルパネル17には、背面側に図示しないコネクタが設けられている。このコネクタは、各種信号を送受信するために機器本体16の前面に設けられた図示しないI/O（Input/Output）ポートに接続される図示しない接続端子と、デタッチセン

【0051】そして、脱着式グリルパネル17が係止手段により機器本体16に装着され、電源端子が接続して脱着式グリルパネル17が機器本体16と電気的に接続状態となると、マイクロコンピュータ31は、デタッチセンサの検知により脱着式グリルパネル17の接続状態を認識する。また、マイクロコンピュータ31は、接続端子の接続により、I/Oポートを介して各種スイッチの設定操作の内容を認識する。なお、脱着式グリルパネル17は、機器本体16と1対1の関係、すなわち他の機器本体16には取り付けできても、この他の機器本体16のマイクロコンピュータ31が所定の対応する脱着式グリルパネル17が装着されていないと判断する構成となっている。

【0052】スピーカ18は、アンプ32から供給され

る増幅された音声信号やアラーム音などの音データを音として出力する。表示装置19は、マイクロコンピュータ31の制御により地図情報などの情報を表示する。

【0053】モーションセンサ12は、従来と同様の構成とされ、車両2の不審（異常）な動きを検知する。すなわち、モーションセンサ12は、例えば、車両2のサスペンションなどに設置され、搭乗者の乗降動作に伴い停止中の車両2が受ける振動のレベルをデータとして管理する。そして、停止中の車両2が牽引車などにより持ち上げられたときに受ける振動など車両2がそのレベルを超える振動を受けたことを検知し、その検知信号をマイクロコンピュータ31に出力する。

【0054】窓割れセンサ13は、従来と同様の構成とされ、車両2に設けられた図示しないドアウィンド、フロントガラス、リアガラスなどが割れたことを検知する。すなわち、窓割れセンサ45は、例えばドアウィンド、フロントガラス、リアガラスなどに埋め込まれており、それらが外部から過度の衝撃を受けたことを検知する。そして、その衝撃力により、フロントガラスなどが割られたと判断してマイクロコンピュータ31に検知信号を出力する。

【0055】認証送受信機14は、例えば、Bluetooth送受信機とされ、上述した無線ユニット33とでデータの送受信を実施するものである。この認証送受信機14にも、マイクロコンピュータ31と同様にして図示しない内蔵メモリが備えられているおり、その内蔵メモリには車両2を所有する所有者（原則として車両2の車検を登録している登録者とされる）の認証コードが予め記憶されてある。

【0056】この認証送受信機14は電子機器11とセットになっており、マイクロコンピュータ31の内蔵メモリに認証コードが設定登録されると、それと同じコード形式で同様の認証コードが記憶される。そして、認証送受信機14は、無線ユニット33との通信が確立されると、その認証コードを示すデータを無線ユニット33に送信する。

【0057】なお、本実施の形態では、この認証送受信機14は、車両2のエンジンの始動やAccスイッチ28をオン/オフするために用いられる車両キー30に取り付けられている。すなわち、車両2を利用する場合に必要な車両キー30に取り付けることで、車両2を利用する際に必ずこの認証送受信機14が携帯されることになり、確実に無線ユニット33との送受信が実施されるようにしている。

【0058】移動通信端末15は、例えば、電子機器11に設けられた図示しないホルダや接続端子などに結合されることで、その電子機器11と接続される携帯電話などの無線通信媒体である。そして、マイクロコンピュータ31の制御により車両2の現在位置を示す位置情報や車両2の異常を示す情報を外部の基地局8に送信す

る。

【0059】なお、車両2に異常が発生した場合に、当該位置情報や異常を示す情報の送信先（基地局8）に関するデータが予め備えられており、マイクロコンピュータ31はそのデータに基づいて移動通信端末15の送信を制御する。さらに、この移動通信端末15は、無線ユニット33との送受信を可能とするBluetooth対応とされている。よって、移動通信端末15が電子機器11に接続されていない状態でも送受信可能な範囲に存在する限り、無線ユニット33との送受信が可能とされ、異常

が発生したことを示す情報を基地局8に送信することができる。

【0060】次に、上記盗難防止システム1の作用を図4に示すフローチャートを参照して説明する。

【0061】まず、ステップ1にて、マイクロコンピュータ31は、車両キー30の操作によりAccスイッチ28がオンされたか否かを判断する。Accスイッチ28がオンされていないと判断した場合には、車両2が走行状態にない、すなわち停止中であると認識する。なお、この状態では、バックアップスイッチ29がオン状態にあるため、マイクロコンピュータ31は、バックアップ（BackUP）電源26からの電力供給により制御処理を実行する。

【0062】次に、ステップ2にて、マイクロコンピュータ31は、窓割れセンサ13からのフロントガラスなどが割れたことを示す検知信号を受けたか否かを判断する。窓割れセンサ13から検知信号を受けていないと判断した場合には、ステップ3に移行し、モーションセンサ12からの所定レベル以上の振動があったことを示す検知信号を受けたか否かを判断する。モーションセンサ12から検知信号を受けていないと判断した場合には、ステップ1に戻り、再度Accスイッチ28がオンされたかの監視を継続する。

【0063】ステップ2にて、窓割れセンサ13から検知信号を受けたと判断した場合、またステップ3にて、モーションセンサ12から検知信号を受けたと判断した場合には、アンプ32を制御して、アラーム音などの音データを生成させる。そして、スピーカ18は、アラーム音などを出力する。

【0064】また、マイクロコンピュータ31は、移動通信端末15が電子機器11に接続されている場合には、その移動通信端末15を制御し、異常が発生したことを示す情報と車両2の現在位置を示す位置情報を基地局8に送信させる。また、移動通信端末15が電子機器11に接続されていない場合には、無線ユニット33を制御し、異常が発生したことを示す情報を移動通信端末15に送信させ、車両2の所有者に報知する。例えば、移動通信端末15に設けられた表示部に異常が発生したことを示す情報を文字情報として表示させることで所有者に報知する。

【0065】基地局8は、盗難防止装置5から送信された異常が発生したことを示す情報と車両2の現在位置を示す位置情報とをネットワーク7を介して監視センタの外部サーバ9に送信する。そして、監視センタは、車両2の位置を特定し、防犯センタである警察署や警備会社などにその特定した位置をネットワーク7を介して報知する。

【0066】一方、ステップ2において、Accスイッチ28がオンされたと判断した場合には、車両2内に搭乗者が存在すると認識する。また、マイクロコンピュータ31は、ステップ4にて、機器本体16がAcc電源25から電力供給を受けて起動状態になったこと、つまり、無線ユニット33が送受信待機状態になったことを認識する（ステップ4）。

【0067】なお、この状態では、バックアップスイッチ29はオフされ、Accスイッチ28のみがオン状態にありAcc電源25から供給される電力によりマイクロコンピュータ31の制御処理が実行される。また、Acc電源25から電力が供給されることにより表示装置19や再生装置などが活性化され起動状態となる。また、脱着式グリルパネル17への電力供給も可能な状態となり、電子機器11全体が活性化される。

【0068】次に、マイクロコンピュータ31は、無線ユニット33から認証コードを示す信号を受けたか否かを判断する。すなわち、認証送受信機14との送受信状態が確立され、その認証送受信機14からの認証コードを示す信号を無線ユニット33が受信したか否かを判断する。受信していないと判断した場合には、再度送受信されたか否かを監視する。

【0069】なお、マイクロコンピュータ31が、例えば、車両2のエンジンが始動されても依然として認証コードを受信していないと判断した場合には、車両2の所有者以外の侵入者により不正に走行されるおそれがある、例えば、違法に車両キー30を複製した侵入者により車両2が盗難されるおそれがあると判断し、アンプ32を制御して、スピーカ18からアラーム音などを出力させるとともに、上述したように、移動通信端末15を制御して基地局8に異常の発生を示す情報と車両2の現在位置を示す位置情報を送信させる。

【0070】認証コードが受信されたと判断した場合には、マイクロコンピュータ31は、次にその受信された認証コードと内蔵メモリに記憶された認証コードとを照合し、一致しているか否かを判断する（ステップ5）。一致していると判断した場合には、正規の所有者により車両2が利用されていると判断して、マイクロコンピュータ31は、アンプ32や移動通信端末15および無線ユニット33を制御することなく、表示装置19や再生装置などを制御して通常の動作を実施させる。

【0071】また、認証コードが一致しないと判断した場合には、所定時間待機し（ステップ6）、所定時間経

っても依然として認証コードが一致しない、すなわち正規の認証コードが受信されないと判断した場合には、上述したように、車両2の所有者以外の侵入者により不正に走行されるおそれがある、例えば、違法に車両キー30を複製した侵入者により不正に走行されるおそれがあると判断し、アンブ32を制御して、スピーカ18からアラーム音などを出力させるとともに、移動通信端末15を制御して基地局8に異常の発生を示す情報と車両2の現在位置を示す位置情報とを送信する。

【0072】なお、車両2が侵入者により不正に走行された場合でも、マイクロコンピュータ31は常に最新の位置情報をGPS受信機22により取得し、それを移動通信端末15を介して基地局8に送信している。そのため、監視センタは、車両2の現在位置を外部サーバ9によりリアルタイムに管理することができ、逐次、防犯センタに車両2の現在位置を通報することで迅速に対処することができる。

【0073】また、ステップ5において、認証コードが一致していると判断した場合、通常動作を実施させる際に、マイクロコンピュータ31は脱着式グリルパネル17が装着されているか否かを判断する(ステップ7)。そして、マイクロコンピュータ31は、脱着式グリルパネル17が装着されていると判断した場合、上述した通常動作を実施させる。

【0074】一方、ステップ7において、脱着式グリルパネル17が装着されていないと判断した場合、所定時間待機し(ステップ8)、所定時間経っても依然として脱着式グリルパネル17が装着されないと判断した場合には、上述したように、車両2の所有者以外の侵入者により不正に走行されるおそれがあると判断し、アンブ32を制御して、スピーカ18からアラーム音などを出力させるとともに、移動通信端末15を制御して基地局8に異常の発生を示す情報と車両2の現在位置を示す位置情報とを送信する。

【0075】上記実施の形態では、以下に示す作用効果を奏する。

【0076】すなわち、車両2にアクセサリ電源25およびバックアップ電源26にて電力が供給されて取り付けられた電子機器11の機器本体16のマイクロコンピュータ31は、認証送受信機14に記憶され車両2の所有者固有の認証コードの信号を認識できない場合に異常が発生したことを示す情報を出力させる。このため、ドアロック解除センサやドア開閉センサなどの車両2の固有の構成を用いることなく、車両2の盗難や車上荒らしなどの異常の発生を確実に防止でき、構造を容易に簡略化でき、車両2毎に異なる構成を用いないので、汎用性を向上できる。さらには、小型化、コストの低減、製造性の向上および設置作業性の向上が容易にできる。

【0077】また、マイクロコンピュータ31が異常の発生を認識することにより、スピーカからアラーム音等

を出力させる。この構成により、電子機器11の構成である再生装置などからの音声信号を出力するスピーカを利用して、車両2の周囲に異常が発生した旨を早期に報知でき、周囲に報知するための特別な構成を用いることなく、盗難や車上荒らしなどを防止できる。

【0078】さらに、車両2の位置情報を取得して電子機器11へ車両2の運行に関する情報信号として出力して画像や音声などで出力させて運行を補助するナビゲーションシステムを設け、このナビゲーションシステムで取得した現在位置情報を異常が発生した旨の信号とともに出力、すなわち報知する。このため、車両2の運行を補助するためのナビゲーションシステムを利用して、異常が発生した旨の信号とともにその位置を報知することができ、盗難の防止や盗難された車両2の位置を容易に認識でき、異常の発生の防止や解決が容易にできる。

【0079】また、異常の発生を認識したマイクロコンピュータ31の制御により、無線ユニット33から異常が発生したことを示す情報を出力させて報知する。このため、車両2から離れた所有者に異常の発生の報知ができるとともに、監視センタや防犯センタへも迅速に異常の発生の報知ができ、異常に対する迅速な対応ができ、利便性も向上できるとともに、遠方からでも車両2を監視でき、盗難などの異常の発生の防止や対処を効率よくできる。

【0080】そして、マイクロコンピュータ31により、認証コードを認識するとともに、電子機器11の機器本体16の動作を設定入力する対応する1つの脱着式グリルパネル17の装着状態を認識し、双方の認識が得られなければ異常と判断するので、近年の巧妙な窃盗などでも多重で利用者を認識する構成により確実に防止でき、誤作動なく確実に利用者を認識できる。

【0081】また、認証コードを送信する認証送受信機14を設け、電子機器11の機器本体16の無線ユニット33にて受信させる構成とする。このため、鍵などではなく、また認証コードを入力操作するなどの作業が不要で、認証コードの照合が、例えば車両2から離れた位置からでもでき、取扱が容易で、利便性を向上できる。

【0082】そして、電子機器11の機器本体16のソースの切替や各種動作制御するためのマイクロコンピュータ31を用いて、車両2の移動や衝撃などによる異常の判断、認証の判別および異常が発生した旨の報知の制御を実施するので、別途特別な構成を用いることなく電子機器11を車両2に取り付けるのみでよく、容易に盗難防止対策ができる。

【0083】また、防犯ネットワーク6に異常の発生を報知する構成としたため、単に異常の発生を早期に認識させることができるとともに、例えば防犯センタに通報するなど、異常に対する適切な対応も迅速にでき、利便性を向上できるとともに、監視センタにて統括して複数の車両2を監視でき、効率よく確実に適切な監視ができ

10

20

30

40

50

る。

【0084】そして、この防犯ネットワーク6への異常の発生は、無線通信媒体を介して報知するので、異常に対して効率よく迅速に対応でき、利便性を向上できるとともに、リアルタイムで遠方からでも監視でき、効率よく確実に適切な監視ができる。

【0085】また、防犯ネットワーク6への異常の発生は、ナビゲーションシステムにて取得した位置情報も報知するので、異常に対して効率よく迅速でより確実に対処できる。

【0086】

【発明の効果】本発明によれば、移動体から供給される電力により機器が起動状態にあるとき、受信した認証コードが記憶された所有者固有の認証コードと一致した場合に移動体の正規の所有者が移動体を利用していると判断するため、ドアロック解除センサやドア開閉センサなどを用いることなく、移動体や移動体に取り付けた機器等の盗難が確実に防止でき、構造が容易に簡略化できるとともに、汎用性を向上できる。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係る盗難防止システムの全体構成を示す概略構成図である。

【図2】前記一実施の形態における取得された車両の位

* 位置情報を蓄積するデータベースの構造を表す模式図である。

【図3】前記一実施の形態における位置情報に基づく画面イメージを表す図である。

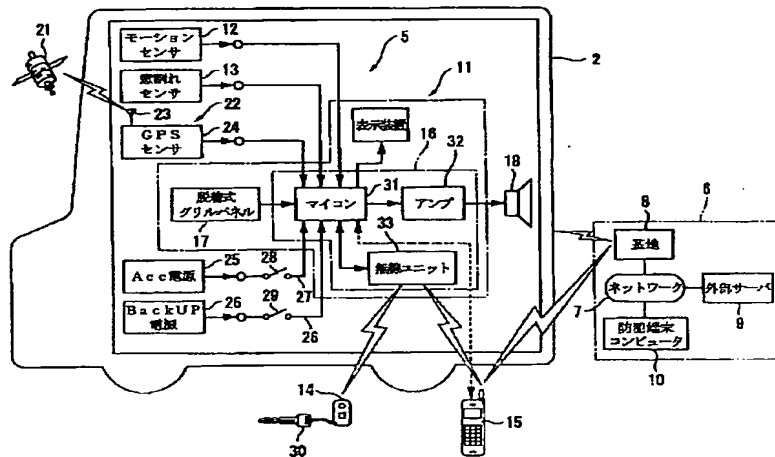
【図4】前記一実施の形態における動作を説明するためのフローチャートである。

【図5】従来例の盗難防止装置を示すブロック図である。

【符号の説明】

- | | | |
|----|----|------------|
| 10 | 1 | 盗難防止システム |
| | 2 | 移動体としての車両 |
| | 5 | 盗難防止装置 |
| | 9 | 外部サーバ |
| | 11 | 電子機器 |
| | 14 | 認証送受信機 |
| | 16 | 機器本体 |
| | 17 | 脱着式グリルパネル |
| | 18 | スピーカ |
| | 22 | GPS受信機 |
| 20 | 25 | アクセサリ電源 |
| | 26 | バックアップ電源 |
| | 31 | マイクロコンピュータ |
| | 33 | 無線ユニット |

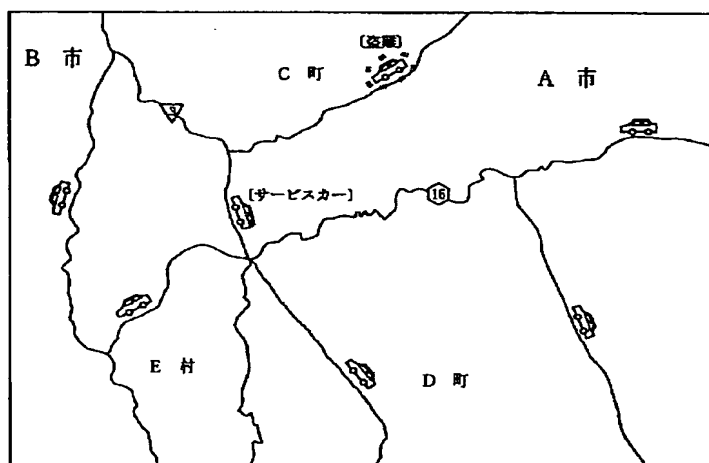
【図1】



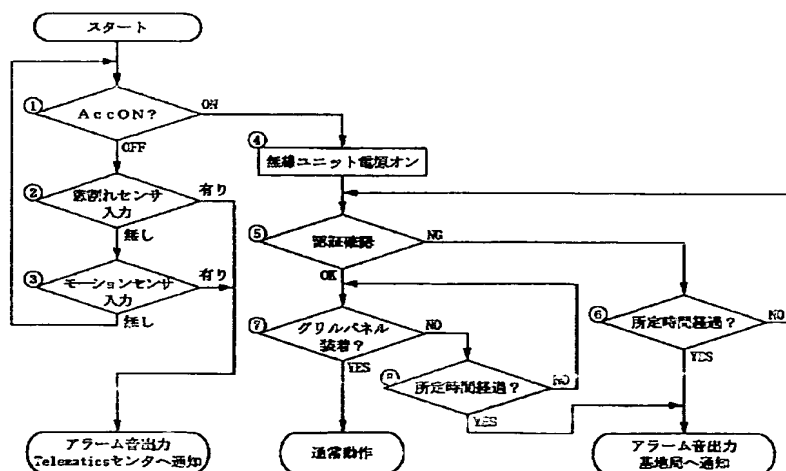
【図2】

| 位置情報DB | | | | |
|--------|----------|-------|-----------|------------|
| 登録番号 | 更新日 | 更新時間 | 位置情報 | |
| | | | 緯度 | 経度 |
| A-0001 | 01/10/01 | 17:00 | N35/43/08 | E142/38/13 |
| A-0002 | 01/10/02 | 17:30 | N35/40/12 | E140/33/17 |
| B-0001 | 01/10/03 | 17:00 | N35/42/15 | E138/42/28 |
| ... | ... | ... | ... | ... |
| ... | ... | ... | ... | ... |
| ... | ... | ... | ... | ... |

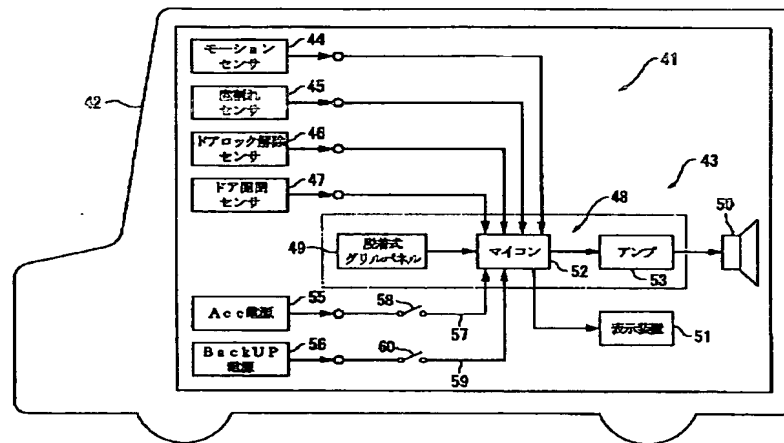
【図3】



【図4】



【図5】



フロントページの続き

| (51)Int.Cl. ⁷ | 識別記号 | F I | ターマコード (参考) |
|--------------------------|-------|---------------|-------------|
| G 0 8 B 25/04 | | G 0 8 B 25/04 | G |
| | | | D |
| H 0 4 Q 9/00 | 3 0 1 | H 0 4 Q 9/00 | 3 0 1 B |
| | 3 2 1 | | 3 2 1 Z |

F ターム (参考) 5C084 AA04 AA09 BB21 CC03 CC08
 CC20 DD79 DD80 EE06 FF02
 FF27 GG43 GG54 HH12 HH13
 5C087 AA02 AA03 AA09 AA24 AA32
 BB12 BB18 BB46 BB65 BB74
 DD05 DD12 EE05 EE16 GG10
 GG19 GG66
 5K048 AA03 AA11 AA15 BA42 BA52
 BA54 DA01 DB01 DC01 EB10
 EB12 FB03 FB11 HA35